contents

ISA-SP18 - Alarm Systems Management and Design Guide

Donald G. Dunn
Principal IEA & Controls Engineer
Lyondell Chemical Company
Channelview, TX 77530

Nicholas P. Sands
Process Control Technology Manager
Chemical Solutions Enterprise
The DuPont Company
Deepwater, NJ 08023

KEYWORDS

Alarm, Alarm System, Alarm Management

ABSTRACT

This paper presents an overview of ISA SP18 effort on an "Alarm Systems Management and Design Guide", a guide that assists individuals, organizations, and suppliers with the application of alarm systems. This document is intended to provide guidance in alarm management for industrial facilities over the entire alarm life cycle from the planning stage, including the development of a philosophy, through the continuous improvement stage, including performance management. This guide documents industry experience and established practices for the application of alarm management and design for application to platforms consisting of programmable electronic systems with processor based graphical user interfaces. This paper gives an overview of the work to date on this topic. Manufacturers, users, and other industry experts have been working since 2003 to develop this consensus guidance.

INTRODUCTION

In October of 2003, at the ISA Expo in Houston, Standards & Practices committee 18 (SP18) started work on an alarm management effort. Since that time, an expanded committee has been assembled that includes vendors, consultants, and users from several different industries. After some time working together the committee has started to produce a draft guidance document. This paper provides a review of the reasons to work on alarm management, the typical problems with alarm systems, and the current status of the SP18 committee's work.

The alarm management effort is important because problems with alarm systems are often cited as contributing factors in industrial incidents. While almost anyone with plant experience knows that alarm management is a common problem, there is still a need to attach a value to the effort. The value varies from site to site and business to business, but the Abnormal Situation Management (ASM) consortium has estimated the cost to US industry at over 13 billion dollars a year.

Presented at ISA EXPO 2005, 25-27 October 2005
McCormick Place Lakeside Center, Chicago, Illinois, www.isa.org

The problems in alarm management are well known. These problems are nuisance alarms, stale alarms, alarm floods and unclear alarms. The solutions to these problems are also known, but they take dedication and discipline to address. The practices essential to an effective alarm management system are described in the alarm management work of SP18. This is still a work in progress.

Several organizations have worked to develop guidance for the design and maintenance of alarm systems. In 1955 ISA formed a survey committee titled Instrument Alarms and Interlocks. The committee evolved to Standard & Practices committee 18. In 1965 the committee completed ISA-RP18.1 *Specifications and Guides for the Use of General Purpose Annunciators*. In 1979 ISA released, as a product of the SP18 and SP67 committees, ISA-18.1-1979 *Annunciator Sequences and Specifications* (1). In 1992 Amoco, Chevron, Exxon, Shell and Honeywell formed the Abnormal Situation Management consortium to develop a vision for better response to plant incidents. In 1999 the Engineered Equipment and Materials Users Association (EEMUA) issued Publication 191, *Alarm Systems: A Guide to Design, Management and Procurement.* In 2003 the User Association of Process Control Technology in Chemical and Pharmaceutical Industries (NAMUR) issued recommendation NA 102 *Alarm Management*.

ALARM SYSTEM PROBLEMS

The most reported problem with alarms systems is nuisance alarms. These are alarms that trigger when no abnormal condition exists or when no operator action is required. Maintenance issues are a frequent cause of nuisance alarms. Because they require no response, these alarms desensitize the operator, and thus reduce the response to real alarms.

Another common problem is stale alarms. Alarms that remain in alarm for extended periods of time because no operator action is required or because they do not clear after operator action has been taken. These alarms build a baseline of clutter in the alarm system masking other alarms from the operator.

One of the most dangerous problems with alarm systems, and the most complex to solve, is the flood of alarms usually associated with an event. These alarm floods overwhelm the operator making it difficult to process the alarms and determine the cause of the event.

One other common problem is a lack of clarity of real alarms. When the cause of the alarm or the response to the alarm is not clear to the operator, the desired action is delayed or not taken and the alarm is ineffective.

PRACTICES

A set of practices has evolved over time to deal with these problems. The EEMUA group, the ASM consortium, and the vendors and consultants that provide alarm management services

deserve significant credit for the development of these practices. These practices, important definitions and reference models are included in the SP18 work.

PURPOSE AND SCOPE

The purpose of the SP18 effort is to define the terminology, models, and processes to effectively implement and manage an alarm system for a process sector facility. The effort is targeted to the process industries but the principles and practices may also be applicable to other industries.

The scope of the effort is limited to computer based alarm systems. The process sensors and final control elements are generally excluded. Safety instrumented systems are excluded except for the alarms generated from those systems. Process data and event data are generally excluded from the standard.

The alarm system consists of the Process Automation System (PAS) and/or Safety Instrumented System (SIS) that generates an alarm message based on measured process conditions or states, the transmission path for the message to the interface for the operator, including the visual and audible annunciation of the message, and the transmission path to the historical repository for the message, including any scheduled reporting or analysis of the message history.

DEFINITIONS

The following are a few of the definitions that are given in the SP18 guide.

alarm: An audible or visible means of indicating to the operator an equipment or process malfunction or abnormal condition (2).

alarm management: The processes and practices for determining, documenting, designing, monitoring, and maintaining alarm messages from process automation and safety systems.

alarm system: The collection of hardware and software that an alarm state, transmits the message to be displayed to the operator, records the message, and generates alarm metric reports.

LIFE CYCLE MODEL

The SP18 committee has placed the existing alarm management practices into a holistic system for managing an alarm system, represented by the life cycle model. The alarm management lifecycle covers the design and maintenance activities from philosophy to management of change. The life cycle model can be useful in identifying the requirements and roles for implementing an alarm management system. This model shows the essential steps, but they may collapse to a simplified model depending on the scope of the alarm system or change and the organizational structure.

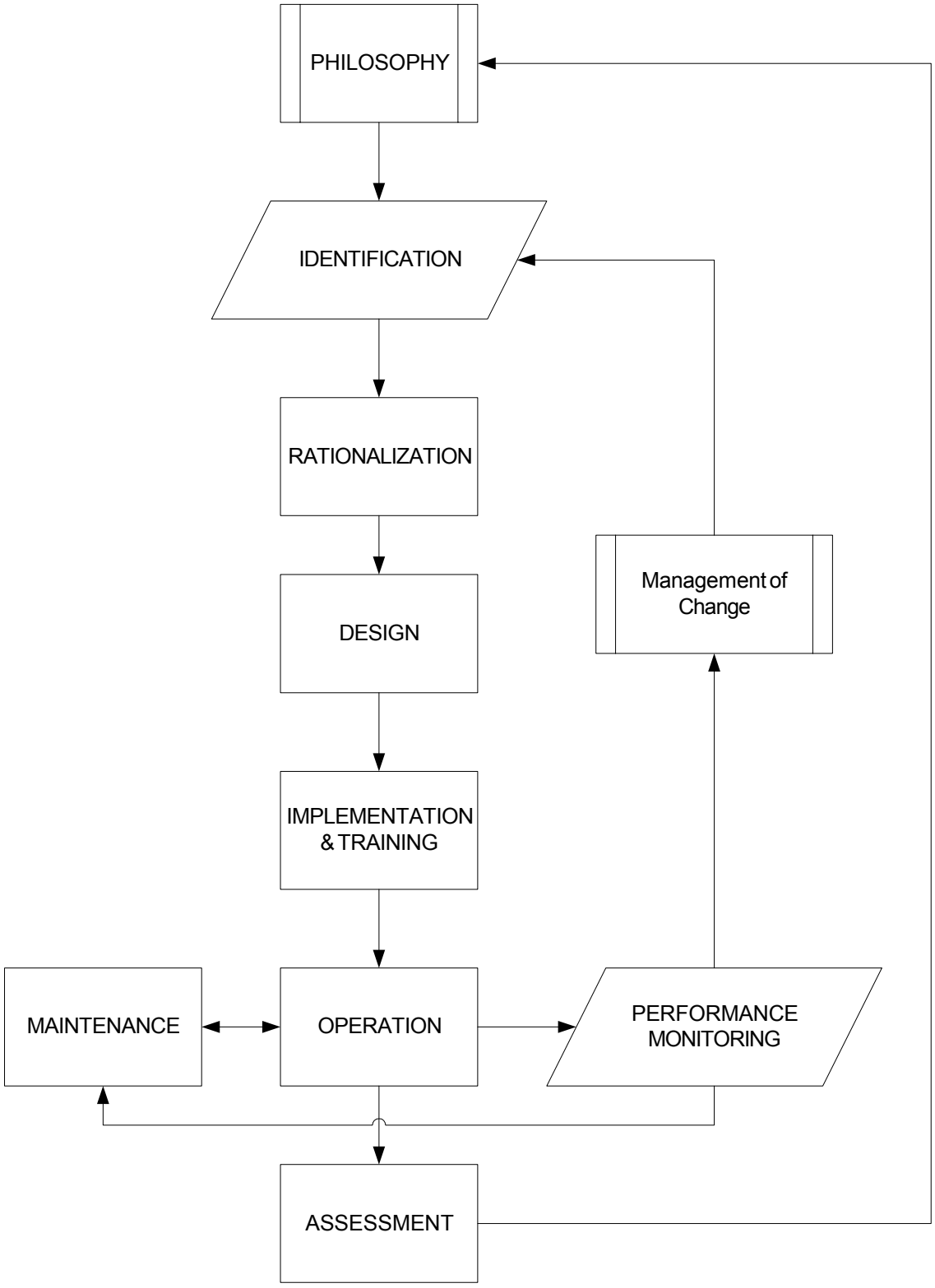

FIGURE 1 – ALARM MANAGEMENT LIFECYCLE

Presented at ISA EXPO 2005, 25-27 October 2005
McCormick Place Lakeside Center, Chicago, Illinois, www.isa.org

PHILOSOPHY

The alarm philosophy documents the site approach to alarm management. It includes the definitions and principles for the alarm system as well as the details of the practices and procedures for each of the remaining life cycle stages. Alarm management improvements without a written philosophy often result in backsliding to pre-improvement performance. The philosophy provides a lasting reference to sustain an effective alarm system.

IDENTIFICATION

Identification of possible alarms can be done by many methods, such as a process hazard analysis or incident investigations. While this is an important step in the life cycle, the methods are not detailed in the work of the SP18 committee, except the identification of problem alarms from routine monitoring. This stage in the life cycle is a holding point for possible alarms to be processed in the next stage.

RATIONALIZATION

Rationalization is the process of reconciling each individual alarm against the principles and requirements of the alarm philosophy and documenting the alarm to support the other stages of the life cycle. The identified possible alarm is reviewed to document the rationale for the alarm, as well as the basic information such as the operator action, response time, and consequence of deviation. This information is critical to improving alarm clarity for the operator.

Once the consequences and the response time have been documented, it is typical to assign the alarm a priority based on a matrix of consequences and priorities. This matrix is defined by the alarm philosophy. Based on the consequences and the safety, regulatory, or policy requirements, the alarm can be classified into design requirement categories capturing such needs as alarm response documentation, alarm retention, and secondary notification requirements like paging or email.

DESIGN

The design stage includes the basic configuration of alarms, the design of the human machine interface (HMI) for alarms, and the advanced methods of alarm management. Each type of design should have a design guide documenting control system specific implementations. The design guide is usually separate from the alarm philosophy, which is mostly system independent. Many nuisance alarms and stale alarms can be eliminated with good basic configuration practices.

IMPLEMENTATION & TRAINING

Presented at ISA EXPO 2005, 25-27 October 2005
McCormick Place Lakeside Center, Chicago, Illinois, www.isa.org

Implementation is the stage where the design is put into service. This process includes training for the operator and initial testing of the alarm system functions. This process is one step in addressing alarm clarity.

OPERATION

Operation is the life cycle stage when the alarm is in service and reporting abnormal conditions to the operator.

PERFORMANCE MONITORING

Performance monitoring is the periodic collection and analysis of data from alarms in the operation life cycle stage. Without monitoring, it is almost impossible to maintain an effective alarm system. This process should take place frequently, perhaps daily or weekly. Monitoring is the primary method to detect problems such as nuisance alarms, stale alarms, and alarm floods.

MAINTENANCE

Maintenance is a necessary step in the alarm life cycle. The process measurement instrument may need maintenance or some other component of the alarm system may need repair. The repair frequency could be scheduled or determined by monitoring. Periodic testing is also a maintenance function. During the maintenance stage, the alarm is not in operation.

ASSESSMENT

Assessment is a periodic audit of the alarm system and the processes detailed in the alarm philosophy. The assessment may determine the need to modify processes, the philosophy, the design guidance, or the need to improve the organization's discipline to follow the processes.

MANAGEMENT OF CHANGE

Management of Change is the structured process of approval and authorization to make additions, modifications, and deletions of alarms from the system. Changes may be identified by many means, including operator suggestions and monitoring. The change process should feed back to the identification stage to ensure that each change is consistent with the alarm philosophy.

ALARM MANAGEMENT LIFECYCLE LOOPS

The life cycle model shows the relationship between the major stages. Included are three loops with significant importance in alarm management. These loops maintain and improve the alarm system.

MONITORING AND MAINTENANCE LOOP

The operation-monitoring-maintenance loop is the daily or weekly process of analyzing the monitored data to determine what unauthorized changes have been made and what instruments need to be repaired. This process can be simple or very complex depending on the automation systems or safety systems used.

MONITORING AND MANAGEMENT OF CHANGE LOOP

The management of change loop is a less frequent, but very necessary process of identifying changes to the alarm system based on analysis of the monitored data. Changes may be identified through other means as well, such as operator suggestions.

Changes to nuisance alarms may be initiated through monitoring. Through monitoring, alarm floods may also be identified. The management of change process can be used to implement advanced alarm management technique to suppress the alarm floods. There is no set frequency for this loop: it happens on demand.

ASSESSMENT LOOP

The assessment-philosophy loop is a periodic audit of the implementation of the alarm philosophy and all of the processes described there. Through audits on training and alarm response, improvements in alarm clarity can be identified as well as changes to the processes and alarm philosophy.

SUMMARY

The life cycle model developed by the SP18 committee puts the known practices of good alarm management together into a framework. These practices address the known problems in alarm systems. The problems of nuisance and stale alarms are addressed with rationalization, good basic configuration and monitoring. The problem of alarm flood is addressed with rationalization, advanced alarm management techniques and monitoring. The problem of alarm clarity is addressed with rationalization, training, HMI design and assessment. The alarm philosophy documents all of the practices so that they can be consistently applied over time.

There is much more to come from the SP18 committee, which is open to more volunteers.

Presented at ISA EXPO 2005, 25-27 October 2005
McCormick Place Lakeside Center, Chicago, Illinois, www.isa.org

REFERENCES

(1) “ISA-18.1 –1979 (R1992) Annunciator Sequences and Specifications”, ISA, Research Triangle Park, North Carolina, July, 1992.

(2) “ISA-RP77.60.02-2000, Fossil Fuel Power Plant Human-Machine Interface: Alarms”, ISA, Research Triangle Park, North Carolina, July, 2000.

Presented at ISA EXPO 2005, 25-27 October 2005
McCormick Place Lakeside Center, Chicago, Illinois, www.isa.org